JAP:NDB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

15 M 0864

- X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

ANY COMPUTER, MOBILE PHONE (829) 508-5868, AND ANY ELECTRONIC DEVICES IN THE CUSTODY OR CONTROL OF JOHNNY VALDEZ

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

- X

EASTERN DISTRICT OF NEW YORK, SS:

DEAN KINSMAN, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is kept and concealed within any computer, mobile phone (829) 508-5868, and any electronic devices in the custody or control of Johnny Santiago Valdez Calderon ("Valdez") (collectively, the "Devices"), the items described in Attachment A to this affidavit, which contain the items described in Attachment B to this affidavit, all of which constitute evidence or the instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud) and 1028A (aggravated identity theft).

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I have been a Special Agent ("Special Agent") with the FBI since May 19, 2002. Since that time, I have been assigned to cybercrime investigations involving numerous cases of computer intrusion, internet fraud, and the theft of intellectual property. The information contained in this affidavit comes from my personal observations and the observations of Task Force Officer ("TFO") Cesar O. Salazar of the Tennessee Bureau of Investigation, FBI SA Carlos Goris and TFO Viviana Gallinal of the Davie, Florida Police Department, my training and experience, information obtained from witnesses, interviews I have conducted, and my examination of reports and records.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1343 (wire fraud) and 1028A (aggravated identity theft) have been committed by the individual described below and by other unknown persons. There is also probable cause to believe that the documents and electronically stored information described in Attachment B is recorded on the Devices as further described in Attachment A.

---

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

I. BACKGROUND

3. The FBI is investigating fraudulent claims submitted to the insurance company Asurion LLC ("Asurion") through Asurion's online Internet portal, www.phoneclaim.com ("web portal"). Asurion is headquartered in Nashville, Tennessee and is engaged in the business of insuring its customers against the loss, theft, or damage of their mobile telephones. To make a claim, an insured submits a claim online and provides personally identifying information, including an insured's name, mobile phone number, and credit card information to pay for the insured's deductible.

4. On September 26, 2014, representatives of Asurion reported to the FBI that they were experiencing high dollar losses annually from fraudulent mobile phone claims. According to Asurion investigators, a user profile must be created on the phoneclaim.com website in order to file mobile phone insurance claims. Asurion representatives advised that unknown subjects ("UNSUBS") were creating thousands of insurance claims on Asurion's web portal requesting that replacement phones be sent to hotel addresses in multiple cities in the United States, as described in greater detail below. Individuals acting as "runners" were suspected to be traveling around the country to pick up the replacement phones at the hotel addresses. One of those UNSUBS has since been identified by the FBI and is described below.

A. INFORMATION FROM COOPERATING WITNESS 1 ("CW-1")

5. On March 15, 2015, an Asurion investigator informed your affiant that on December 12, 2014 an individual, hereinafter referred to as Cooperating Witness 1 ("CW-1"),

was arrested in North Charleston, South Carolina, for receiving approximately 100 fraudulent mobile phone shipments from Asurion.

6. On March 18, 2015, Detective Charlie Benton of the North Charleston Police Department provided to your affiant the Incident and Evidence Inventory Reports regarding the arrest of CW-1 under the fake name "Kevin Garcia." Your affiant reviewed the above mentioned reports and learned that on December 12, 2014 Detective Benton received information from the management at the North Charleston Inn, located at 2934 West Montague Avenue, North Charleston, SC regarding suspicious activity involving their location and other locations managed by the same operations group. The management of the North Charleston Inn told Detective Benton, that an individual by the name of "Kevin Garcia" ("Garcia") had reservations at several area hotels, including the North Charleston Inn, which were accompanied by United Parcel Service ("UPS") deliveries for the same individual on the date of the reservation.

7. According to those reports, Garcia would make reservations at the different hotels and advise hotel staff that he expected to receive packages there. Garcia never confirmed his reservations, nor did he check into the hotels. Garcia would later return to receive the packages, and upon receipt, he would offer an excuse for leaving and express his intention to return later. Garcia did not return and any charges attempted by the hotels against his credit card were denied. Hotel management advised that all the packages came from a company named Asurion in Tennessee. Management for the operations group saw that "Kevin Garcia" had an unconfirmed reservation for December 12, 2014 at the North Charleston Inn.

8. On December 12, 2014, Detective Benton responded to the North Charleston Inn and witnessed CW-1 take ownership of two packages from Asurion which were addressed to "Kevin Garcia." When CW-1 was questioned about his identity, he stated that Kevin Garcia was not his real name and that the New Jersey driver's license under the same name bearing his photograph was fraudulent. CW-1 stated that he traveled to the area to pick up phones to re-ship to the Dominican Republic. At the time of his arrest, CW-1 had in his possession approximately 100 phones from Asurion. CW-1 was arrested on charges of Obtaining Goods by False Pretense, Drug/Narcotics Violations, and Obstruction of Justice.

9. On April 22, 2015, your affiant, TFO Cesar O. Salazar, and Detective Benton interviewed CW-1 in the presence of his attorney. CW-1 admitted that he had been a runner picking up mobile phones at multiple cities in the United States since late 2013. The phones he picked up were replacement devices shipped pursuant to fraudulent insurance claims submitted on Asurion's web portal. CW-1 stated that he received his instructions from an individual by the name "Johnny Santiago Valdez Calderon" ("Valdez") residing in the Dominican Republic. CW-1 stated that he has personally met with Valdez in the Dominican Republic on several occasions.

10. According to CW-1, Valdez has a group of approximately 21 individuals working for him who submit fraudulent claims on the Asurion web portal. Valdez also made reservations in a number of hotels in a particular city under a fictitious name. The fictitious name and address of the hotels were used for the delivery of the fraudulently-obtained mobile phones. Working with CW-1, Valdez would then mail a fraudulent driver's license to CW-1 bearing a photograph

of CW-1 and also email the hotel names and addresses to CW-1. In the North Charleston case, CW-1 was using the fake name and driver's license of Kevin Garcia.

11. According to CW-1, after CW-1 received the mobile phones, he sold them for cash. CW-1 tasked his spouse with sending the majority of the money to Valdez via money transfer services such as Western Union and Moneygram. CW-1 kept approximately $50 from every phone he sold as payment for his participation in the scheme. CW-1 and his spouse were transferring so much money to Valdez via Western Union that Western Union became suspicious and refused to allow CW-1's spouse to send money. Consequently, in one instance, CW-1 asked a friend who was travelling to the Dominican Republic to deliver money to Valdez in person. CW-1's friend had never previously met Valdez in person. Prior to their meeting, Valdez sent CW-1 a picture of Valdez so CW-1's friend could identify Valdez.

12. After CW-1's friend delivered the money to Valdez in the Dominican Republic, Valdez sent CW-1 a photograph of himself holding the money to confirm his receipt. In addition, due to Western Union's refusal to conduct further business with CW-1's spouse, on November 7, 2014, CW-1 transferred by wire $4,685 to a bank account bearing an account number ending in 6693 and in the name of Johnny Santiago Valdez Calderon at Banco Popular in the Dominican Republic. On several occasions, CW-1 personally travelled to the Dominican Republic to deliver to Valdez cash proceeds from CW-1's sale of phones received from Asurion.

13. On May 11, 2015 and June 8, 2015, your affiant obtained from Western Union and Moneygram records showing that between April 22, 2014 and October 25, 2014, CW-1 or his spouse sent $65,781 to Valdez. The records also show that Valdez received the money using

a Dominican Republic state-issued identification bearing his date of birth of October 10, 1992, and the address C/ Principe Negro #78, El Rosal, Santo Domingo Este in the Dominican Republic (the "Valdez Residence"). Valdez also provided his telephone number of (829) 508-5868 when he received the funds.

B. COMMUNICATION BETWEEN CW-1 AND VALDEZ

14. The primary means of communications between CW-1 and Valdez were via email and the text messaging smartphone application WhatsApp, a free service. WhatsApp is a cross-platform mobile messaging app, similar to text messaging, which allows a user to exchange messages through a data plan without having to pay for each SMS message by associating a mobile phone number with a WhatsApp account. In addition to basic messaging, WhatsApp users can create groups, and send shared images, video and audio media messages.

15. According to CW-1, Valdez used his mobile telephone number of (829) 508-5868 to send messages from his WhatsApp account. The telephone number (829) 508-5868 is the same number which is noted in Western Union's money transfer records as belonging to Valdez. CW-1 also provided written consent to obtain a copy of the contents of his iCloud account, his mobile phone and his laptop computer. iCloud is an online service offered by Apple, Inc., which can function as a backup destination for smartphone users, including backups of WhatsApp data. On April 24, 2015 TFO Salazar copied the contents of CW-1's iCloud account, including email messages and WhatsApp data.

16. On May 7, 2015 TFO Salazar conducted a cursory review of the email messages between CW-1 and Valdez and found approximately 70 email messages concerning the scheme from Valdez to CW-1. Specifically, TFO Salazar discovered an email dated December 12, 2014, from the email address "almacen829@gmail.com" to an email address which belongs to CW-1 with the subject line "track viernes." "Viernes" is the Spanish word for "Friday." The body of the email message listed 16 smart phone models, UPS tracking numbers, the hotel names and addresses for receipt of each phone, in the name Kevin Garcia. One of the hotels listed was the North Charleston Inn, 2934 W. Montague Ave, North Charleston, SC 29418, which is the hotel and address where CW-1 was arrested. According to CW-1, Vadez used two email addresses, "almacen829@gmail.com" and "almacen849@gmail.com" to communicate with CW-1 about the scheme.

17. On May 7, 2015 TFO Salazar conducted a further review of the photos and audio files downloaded from CW-1's iCloud account and found numerous images and audio files exchanged between CW-1 and phone number (829) 508-5868, which was used by Valdez. Several images depicted screen shots of lists of addresses, UPS tracking numbers, and mobile phone models. These images were consistent with the email messages received by CW-1 from "almacen829@gmail.com" for the purpose of picking up mobile phones from Asurion.

18. On May 14 and May 26, 2015, TFO Salazar executed search warrants on the e-mail accounts "almacen829@gmail.com" and "almacen849@gmail.com." Both accounts contained thousands of e-mail communications exchanged between Valdez and his organization,

revealing a widespread conspiracy involving the submission of fraudulent mobile phone claims on the Asurion web portal using fraudulent identity documents such as altered U.S. passports.

19. If Asurion suspects a submitted claim might not be genuine, Asurion customer service personnel request that the claimant 1) submit an affidavit describing how the insured device was lost, stolen or damaged, 2) submit a copy of a government-issued identification document, and 3) answer various security questions intended to verify the claimant's identity before a replacement mobile phone is shipped to the claimant. The review of the emails in e-mail accounts "almacen829@gmail.com" and "almacen849@gmail.com" also revealed file attachments that contain Asurion claim numbers, profile names, mobile phone models, shipping addresses, shipment tracking numbers and the source of the profile information such as Instantcheckmate.com. Several spreadsheets saved within the "almacen829@gmail.com" and "almacen849@gmail.com" accounts contain what appear to be records of payments made by Valdez to various members of his organization.

20. From your affiant's training an experience, he knows that Instantcheckmate.com is a publicly accessible website that provides reports consolidated from public records and court documents. Some Instantcheckmate.com records contain names, addresses, and telephone numbers, which can be accessed by a user, for a fee.

21. In May of 2015, at the request of your affiant, CW-1 again contacted Valdez on his WhatsApp account to request that Valdez file fraudulent claims on the Asurion web portal and initiate shipments to CW-1. On May 7, 2015, Valdez told CW-1 to send to him a picture of himself so Valdez could create fraudulent identification documents using the website

www.idninja.net. Valdez created fraudulent identification documents in the names "Carlos Mendoza", "David Rodriguez," and "Luis Encarnacion" using CW-1's picture and mailed them to CW-1. After CW-1 received the fraudulent identification documents, Valdez or a member of his organization initiated claims on the Asurion web portal resulting in the shipment of eight mobile phones to various hotels and UPS stores. Valdez sent the tracking numbers to CW-1 through a WhatsApp message. CW-1 received the same information in an email sent from the e-mail address "luisencarnacion1@mail.com."

22. On June 2 and 4, 2015, CW-1 received all eight mobile phones. On June 4, 2015, SA Goris and TFO Gallinal met CW-1 and took custody of the mobile phones CW-1 received and the boxes they were shipped in. The tracking numbers on the boxes and mobile phone models matched the models and tracking numbers Valdez sent to CW-1 via WhatsApp and in the e-mail from the address "luisencarnacion1@mail.com."

23. On June 10, 2015, Valdez sent CW-1 a WhatsApp message containing a screenshot of his computer displaying a spreadsheet with the tracking numbers, phone models and amounts of money he expected to receive from CW-1 for the mobile phone shipments he initiated at CW-1's request and received by CW-1 on June 2 and 4, 2015. According to the spreadsheet, Valdez expected CW-1 to send $2,750 to him for the mobile phones. On June 16, 2015, SA Goris and TFO Gallinal met CW-1 and provided him the money Valdez requested. CW-1 proceeded to a Moneygram location and initiated a transaction to transfer money to Valdez in the Dominican Republic in the amount of $2,750.

24. On June 4, 2015, CW-1 received another e-mail from the account "luisencarnacion1@mail.com" containing five mobile phone models and shipping addresses for fraudulent claims Valdez or a member of his organization had filed on the Asurion web portal. On June 16, 2015, CW-1 received all five mobile phones noted in the email.

25. On June 18, 2015, Valdez sent CW-1 a WhatsApp message containing a photograph from a mobile phone displaying the mobile phone models and amounts of money he expected to receive from CW-1 for the mobile phone shipments which CW-1 received on June 16. According to the photograph, Valdez expected CW-1 to send $1,690 to him for the mobile phones. On June 19, 2015, SA Goris and TFO Gallinal met CW-1 and took custody of the mobile phones CW-1 received and the boxes they were shipped in. The shipping addresses on the boxes and mobile phone models matched the models and addresses which Valdez sent CW-1 via e-mail. SA Goris and TFO Gallinal provided CW-1 the money Valdez requested. CW-1 proceeded to a Moneygram location and initiated a transaction to transfer money to Valdez in the Dominican Republic in the amount of $1,690.

26. On June 16, 2015, your affiant requested from Asurion any information involving claims filed with Asurion that are associated with the information contained in the e-mail accounts "almacen829@gmail.com" and "almacen849@gmail.com." Your affiant provided a copy of the "almacen829@gmail.com" and "almacen849@gmail.com" e-mail search warrant proceeds to Asurion. According to documents provided to your affiant by Asurion, the e-mail accounts "almacen829@gmail.com" and "almacen849@gmail.com" are directly associated with approximately $734,933 in losses from fraudulent mobile phone shipments between July 23,

2104 and May 27, 2015 and approximately $245,620 in fraudulent credit card charges submitted to pay the amounts of the deductibles on the fraudulent insurance claims filed.

27. Based on records provided by Asurion, your affiant contacted M.C., a resident of the Middle District of Tennessee whose name, address, and mobile phone number ***-***-4469 had been used to file a fraudulent claim on the Asurion web portal. M.C. confirmed that she did not file a claim with Asurion nor did she authorize anyone to file a claim on her behalf.

28. Based on records provided by Asurion, your affiant contacted J.S.H.J, a resident of the Middle District of Tennessee whose name, address, and mobile phone number ***-***-0004 had been used to file a fraudulent claim on the Asurion web portal. J.S.H.J confirmed that he did not file a claim with Asurion nor did he authorize anyone to file a claim on his behalf.

29. On June 27, 2015, your affiant used forensics software to extract the WhatsApp chats between Valdez and CW-1 from CW-1's mobile phone. The chats contain over 400 pages of messages and voice recordings in Spanish exchanged between Valdez and CW-1. In some of those messages, Valdez instructs CW-1 on the location of mobile phone packages sent by Asurion, and the amounts of money Valdez expects to receive from CW-1 for the sale of the phones. On November 13, 2014, Valdez instructed CW-1 to send information surrounding his receipt of packages from Asurion to the e-mail address "almacen829@gmail.com."

30. According to records obtained from Google, Inc., on January 4 and 5, 2015, Valdez sent two e-mails from "almacen849@gmail.com" to almacen849@gmail.com. The substance of those two emails appears intended for an unidentified group of approximately

fifteen co-conspirators instructing them how to complete online profiles for damaged cell phone claims and how to organize and store profile information in folders on their computer system. The same e-mails also provided the usernames for use of the websites SSBDOB.so, Intelius and InstantCheckmate.com, and listed prices for various mobile phone models.

31. From your affiant's training an experience, he knows Intelius, like Instantcheckmate, provides reports consolidated from public records and court documents. Some Instantcheckmate.com records contain addresses, and telephone numbers that can be accessed for a fee. Valdez advised the e-mail recipients that there are fifteen members in their organization, and future e-mails containing Asurion claim data should be sent to "almacen849@gmail.com."

C. IDENTIFICATION OF VALDEZ

32. On May 7, 2015, your affiant contacted SA Karen Turner of the U.S. State Department and requested copies of any records in the possession of the U.S. State Department under the name Johnny Santiago Valdez Calderon. SA Turner responded via e-mail by enclosing a copy of Valdez' application for a U.S. passport dated October 12, 2011. The application was filed in the name of Johnny Santiago Valdez Calderon and contained a photograph of Valdez that appears to depict the same individual depicted in the photographs of himself that Valdez provided to CW-1. According to Valdez' passport application, he was born on October 10, 1992 in Brooklyn, New York. A copy of Valdez' U.S. birth certificate was also enclosed with his passport application. At the time of his application, he resided at the Valdez Residence in the Dominican Republic and previously held a U.S. passport.

33. On May 20, 2015, FBI Assistant Legal Attaché ("ALAT") Sean Haworth, assigned to the U.S. Embassy in Santo Domingo, Dominican Republic sent your affiant a credit report from Caltec Scoring Technologies in the name of Johnny Santiago Valdez Calderon. According to this report, Valdez was born on October 10, 1992 in Brooklyn, New York, uses mobile telephone number (829) 508-5868, and as of April 10, 2015, he resided at the Valdez Residence in the Dominican Republic. The report contained a photograph of Valdez that appears to depict the same individual depicted in the photographs of himself that Valdez provided to CW-1 and the photo contained in Valdez' passport application previously described.

34. According to public records, the mobile telephone service provider for (829) 508-5868 is Claro Codetel. On July 6, 2015, ALAT Haworth received subscriber records for telephone number (829) 508-5868 from Claro Codetel. According to Claro Codetel records, telephone number (829) 508-5868 is assigned to Johnny Valdez Calderon and Calderon resides at the Valdez Residence in the Dominican Republic.

D. VALDEZ' TRAVEL TO THE UNITED STATES

35. On August 19, 2015, your affiant discovered a Facebook account for a user named Prissilia Mena displaying a profile picture posted on June 24, 2015 which shows Valdez posing with a female who appears to be Mena. In the profile picture, Mena appears to be approximately six months pregnant. On August 20, 2015, your affiant received information from CW-1 that Valdez was travelling to the U.S. to accompany his girlfriend Prissilia Mena during the birth of their baby. Valdez' girlfriend was due to give birth on October 3, 2015, and Valdez intended to arrive in New York sometime in September 2015. Your affiant contacted Homeland

Security Investigations ("HSI") Special Agent Wayne Dickey who confirmed Prissilia Mena arrived in New York's John F. Kennedy airport on July 25, 2015. SA Dickey put an alert in Homeland Security's computer system to notify him if Valdez made arrangements to travel to the United States or Mena made arrangements to leave the United States.

36. On September 7, 2015, CW-1 contacted Valdez and was advised by Valdez that his girlfriend now was due to give birth on September 22, 2015 that that Valdez intended to arrive in the United States by Friday, September 11, 2015.

37. On September 8, 2015, CW-1 was advised by Valdez that he had reserved a seat on a JetBlue Flight leaving Santo Domingo at 6:00 a.m. on Friday, September 11, 2015. I confirmed through online resources that JetBlue Flight 310 is scheduled to leave Santo Domingo at 6:00 a.m. on Friday, September 11, 2015 and is scheduled to arrive at JFK International Airport in New York City at 9:48 a.m. that same date.

38. On September 9, 2015, SA Dickey advised that Valdez was scheduled on JetBlue Flight 410 to leave Santo Domingo later on Friday, September 11, 2015 and scheduled to arrive at JFK International Airport in New York City at 8:25 p.m. that evening. ⊗

39. From your affiant's training and experience, he believes Valdez intends to stay in the United States for several weeks in order to accompany Mena. From your affiant's review of the Almacen829@gmail.com and Almacen829@gmail.com accounts, there is fraudulent e-mail activity nearly every day in these accounts, therefore, Valdez will likely attempt to continue

⊗ Due to the arrival time's proximity to 10 p.m., it is likely that agents will not be able to execute the warrant ~~after~~ before 10 p.m. CP DK

fraudulent activity toward Asurion during the time he is in the United States. In order to do so, Valdez will likely travel with a laptop computer and mobile telephone.

II. PROBABLE CAUSE TO BELIEVE THAT VALDEZ' PERSON AND BAGGAGE CONTAIN ELECTRONIC DEVICES AND STORAGE MEDIA THAT CONTAIN EVIDENCE, FRUITS, OR INSTRUMENTALITIES OF CRIMINAL ACTIVITY

40. In my experience, individuals who are traveling typically make arrangements to have a relative or acquaintance meet them at their port of arrival for transportation to their final destination. Upon arrival, the traveler will call his acquaintance to agree upon a meeting point. In addition, individuals traveling overseas on multi-week travel typically bring with them, and carry on their person and store in their luggage a variety of items, including electronic devices, such as iPads or other tablet devices, cell phones, and laptop computers, as well as electronic storage media. Some of these electronic devices, such as a cell phone, are small enough to fit in a pocket or carrying bag such as a purse. Additionally, individuals who are traveling internationally for extended periods will typically carry identification documents such as passports or driver's licenses to provide proof of their identity and the legitimacy of their term in the travel destination.

41. Therefore, based upon the information above, I submit that there is probable cause to believe that Valdez will likely travel to a New York area airport to meet Mena, he has violated Title 18, United States Code, Sections 371, 1343, and 1028A, and he likely will have a mobile smartphone, or other electronic communication device, laptop computer or electronic storage device on his person or in his baggage which contains evidence of his online conduct related to the online scheme.

III. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on a device. This information can sometimes be recovered with forensics tools.

43. As described above and in Attachment B, this application seeks permission to search for records that might be found on the person of Valdez, in whatever form they are found. One form in which records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

44. *Probable cause.* I submit that if a computer or storage medium is found on the person of Valdez, there is probable cause to believe such records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

45. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created.

The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

46. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic

electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

48. *Manner of execution.* Because this warrant seeks only permission to examine a device and storage media that will be found on the person or in his control, as described in Attachment A, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

III. CONCLUSION

49. Based upon the information above, I submit that there is probable cause to believe that Valdez has violated Title 18, United States Code Sections 1343, and 1028A, and further there is probable cause to believe that Valdez will carry on his person or baggage one or more electronic communications devices when he arrives in a New York area airport, which Devices are likely to contain evidence of criminal activity. Therefore, I request a search warrant authorizing the search of any electronic communications device, laptop computer or storage media as well as an examination of any such electronic devices on his person or in such baggage, as described in Attachment A, to seek the items described in Attachment B.

50. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in

that it might alert the target(s) of the investigation and likely lead to the destruction and concealment of evidence, and/or flight. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for ANY COMPUTER, MOBILE PHONE (829) 508-5868, AND ANY ELECTRONIC DEVICES IN THE CUSTODY OR CONTROL OF JOHNNY VALDEZ.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

Respectfully submitted,

Special Agent Dean Kinsman
Federal Bureau of Investigation

Sworn to before me on this 10 day of September 2015

THE HONORABLE CHERYL L. POLLAK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The property to be searched is any electronic communications device, mobile phone (829) 508-5868, laptop computer or electronic storage media as well as an examination of any such electronic devices on his person or in such baggage belonging to Johnny Santiago Valdez Calderon (collectively, the "Devices"). This warrant authorizes the forensic examination of any Devices and storage media found on Valdez' person or in such baggage for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, United States Code, Sections 1343 and 1028A, those violations occurring after January 1 2013, including:

a. Records and information relating to a conspiracy to defraud Asurion;

b. Records and information relating to the filing of fraudulent insurance claims on the Asurion web portal;

c. Records and information relating to Asurion;

d. Records and information relating to the e-mail accounts almacen829@gmail.com, and almacen849@gmail.com and other co-conspirators.

e. Records and information relating to the WhatsApp account utilized by mobile telephone number (829) 508-5868 and other co-conspirators.

f. Records and information relating to the identity or location of the suspects;

g. Records and information relating to money transfers services such as Western Union and Moneygram.

2. Computers, mobile telephones or storage media used as a means to commit the violations described above, including the filing of fraudulent mobile phone insurance claims and receipt of funds related to the filing of fraudulent mobile phone insurance claims in violation of 18 U.S.C. § 1343 and § 1028A.

3. For any computer, mobile telephone or storage medium whose seizure is otherwise authorized by this warrant, and any computer, mobile telephone or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.